

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2002-244756
(P2002-244756A)

(43)公開日 平成14年 8 月30日 (2002. 8. 30)

(51)Int.Cl. ⁷	識別記号	F I	ページ* (参考)
G 0 6 F 1/00		G 0 6 K 17/00	D 5 B 0 3 3
G 0 6 K 17/00			E 5 B 0 5 8
19/07		G 0 9 C 1/00	6 4 0 A 5 B 0 7 6
19/073		G 0 6 F 9/06	6 6 0 C 5 J 1 0 4
			6 6 0 J
審査請求 未請求 請求項の数20 O L (全 14 頁) 最終頁に続く			

(21)出願番号 特願2001-42396(P2001-42396)

(22)出願日 平成13年 2 月19日 (2001. 2. 19)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川 6 丁目 7 番35号

(72)発明者 末吉 正弘

東京都品川区北品川 6 丁目 7 番35号 ソニ
ー株式会社内

(72)発明者 久保野 文夫

東京都品川区北品川 6 丁目 7 番35号 ソニ
ー株式会社内

(74)代理人 100094053

弁理士 佐藤 隆久

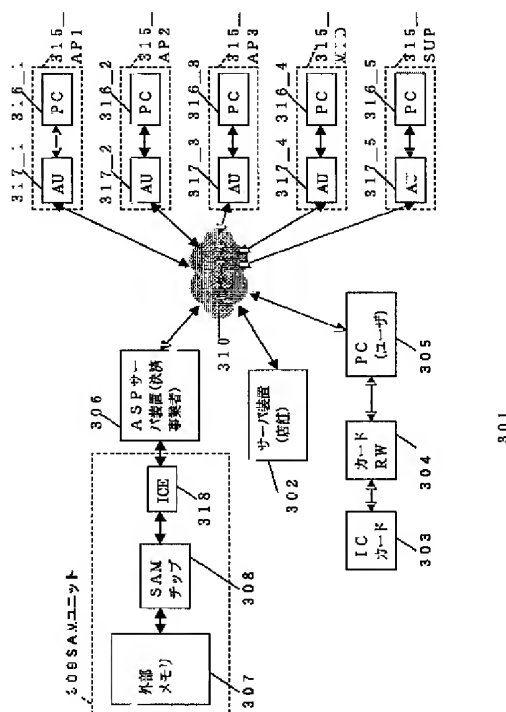
最終頁に続く

(54)【発明の名称】 データ処理方法、半導体回路および認証用装置

(57)【要約】

【課題】 サーバ装置などの半導体回路へのアクセス内容をその権限に応じて規制できるデータ処理方法を提供する。

【解決手段】 SAMチップ308が、複数の階層からなるソフトウェア構造を有し、各階層に対応したダウンロード用署名検証鍵情報参照可能である。SAMチップ308がパーソナルコンピュータ316_1からダウンロード要求を受けると、認証用ユニット317_1において、ダウンロード用署名情報を作成し、これがSAMチップ308に送信される。SAMチップ308では、ダウンロード用署名検証鍵情報を用いて、受信したダウンロード用署名情報を検証し、正当であると判断した場合にダウンロードを認める。



【特許請求の範囲】

【請求項1】半導体回路または当該半導体回路がアクセス可能な半導体記憶装置に、前記半導体回路内で動作するプログラムをダウンロードするデータ処理方法において、

前記半導体回路が複数の階層からなるソフトウェア構造を有し、各階層に対応したダウンロード用署名検証鍵情報を前記半導体回路が参照可能であり、

前記半導体回路がダウンロード要求を受けると、当該ダウンロード要求に対応して生成されたダウンロード用署名情報を、前記ダウンロード用署名検証鍵情報を用いて検証し、

前記ダウンロード用署名情報が正当であると検証したことを条件に、当該検証に用いたダウンロード用署名検証鍵情報に対応した階層プログラムのダウンロードを、前記ダウンロード要求の発行元に許可するデータ処理方法

【請求項2】認証用装置が、ダウンロードが許可されるプログラムが属する階層に対応したアクセス原鍵情報を記憶し、

前記認証用装置が、前記半導体回路に前記ダウンロード要求を送信し、

前記認証用装置が、当該アクセス原鍵情報を用いて前記ダウンロード用署名情報を生成し、当該ダウンロード用署名情報を前記半導体回路に送信する請求項1に記載のデータ処理方法。

【請求項3】前記認証用装置が、前記半導体回路の識別情報を記憶し、

前記認証用装置が、前記識別情報を平文として前記アクセス原鍵情報を用いて暗号化を行ってダウンロード用原鍵情報を生成し、当該ダウンロード用原鍵情報を用いて前記ダウンロード用署名情報を生成する請求項2に記載のデータ処理方法。

【請求項4】前記認証用装置が、前記半導体回路へのダウンロードを許可された前記階層に対応する第1のアクセス原鍵情報、並びに、当該階層の上位の単数または複数の階層にそれぞれ対応した単数または複数の第2のアクセス原鍵情報を記憶し、

前記認証用装置が、前記第1のアクセス原鍵情報、並びに前記単数または複数の第2のアクセス原鍵情報を用いて前記ダウンロード用署名情報を生成する請求項2に記載のデータ処理方法。

【請求項5】前記認証用装置は、前記半導体回路との間で相互認証を行った後に、前記ダウンロード用署名情報を前記半導体回路に送信する請求項2に記載のデータ処理方法。

【請求項6】前記認証用装置が、相互認証用原鍵情報、並びに前記半導体回路の識別情報を記憶し、

前記認証用装置が、前記識別情報を平文として前記相互認証用原鍵情報を用いて暗号化を行って相互認証用鍵情報を生成し、

前記認証用装置が、前記相互認証用鍵情報を用いて前記半導体回路との間で相互認証を行う請求項5に記載のデータ処理方法。

【請求項7】前記半導体回路のソフトウェア構造が、前記半導体回路の管理者にのみダウンロード権が与えられた第1の階層と、前記第1の階層の上位に位置し所定の集積回路を操作するプログラムが属する第2の階層と、前記第2の階層の上位に位置し前記集積回路を用いた取り引き手続き内容を規定したアプリケーションプログラムが属する第3の階層とに分類されている請求項1に記載のデータ処理方法。

【請求項8】前記集積回路は、カードに搭載されており、

前記半導体回路は、通信回線、並びに当該通信回線に接続された通信装置を介して前記集積回路にアクセスを行う請求項8に記載のデータ処理方法。

【請求項9】前記第3の階層には、前記集積回路を用いた取り引きを行う複数の事業者のそれぞれに対応したアプリケーションプログラムが属し、当該複数のアプリケーションプログラムのそれぞれにファイアウォールが規定されており、前記ファイアウォールを介した前記アプリケーションプログラム間のデータ授受またはデータ参照が規制されている請求項8に記載のデータ処理方法。

【請求項10】前記認証用装置は、当該認証用装置に加えられた物理的な外力であって前記アクセス原鍵情報が不正に操作される可能性がある外力を検出した場合に、前記記憶しているアクセス原鍵情報を自動的に消去する請求項2に記載のデータ処理方法。

【請求項11】複数の階層からなるソフトウェア構造を有する半導体回路であって、

各階層に対応したダウンロード用署名検証鍵情報を参照可能であり、ダウンロード要求を受けると、当該ダウンロード要求に対応して生成されたダウンロード用署名情報を、前記ダウンロード用署名検証鍵情報を用いて検証し、

前記ダウンロード用署名情報が正当であると検証したことを条件に、当該検証に用いたダウンロード用署名検証鍵情報に対応した階層のプログラムを、当該半導体回路または当該半導体回路にアクセス可能な半導体記憶回路にダウンロードすることを、前記ダウンロード要求の発行元に許可する半導体回路。

【請求項12】前記半導体回路のソフトウェア構造が、前記半導体回路の管理者にのみダウンロード権が与えられた第1の階層と、前記第1の階層の上位に位置し所定の集積回路を操作するプログラムが属する第2の階層と、前記第2の階層の上位に位置し前記集積回路を用いた取り引き手続き内容を規定したアプリケーションプログラムが属する第3の階層とに分類されている請求項12に記載の半導体回路。

【請求項13】前記集積回路は、カードに搭載されてお

り、

前記半導体回路は、通信回線、並びに当該通信回線に接続された通信装置を介して前記集積回路にアクセスを行う請求項13に記載の半導体回路。

【請求項14】前記第3の階層には、前記集積回路を用いた取り引きを行う複数の事業者のそれぞれに対応したアプリケーションプログラムが属し、当該複数のアプリケーションプログラムのそれぞれにファイアウォールが規定されており、前記ファイアウォールを介した前記アプリケーションプログラム間のデータ授受またはデータ参照が規制されている請求項14に記載の半導体回路。

【請求項15】複数の階層からなるソフトウェア構造を有する半導体回路または当該半導体回路がアクセス可能な半導体記憶装置に、前記半導体回路内で動作するプログラムをダウンロードする際の認証に用いられる認証用装置であって、

前記ダウンロードが許可されるプログラムが属する前記階層に対応したアクセス原鍵情報を記憶し、
前記半導体回路に前記ダウンロード要求を送信し、
当該アクセス原鍵情報を用いて前記ダウンロード用署名情報を生成し、当該ダウンロード用署名情報を前記半導体回路に送信する認証用装置。

【請求項16】前記半導体回路の識別情報を記憶し、
前記識別情報を平文として前記アクセス原鍵情報を用いて暗号化を行ってダウンロード用原鍵情報を生成し、当該ダウンロード用原鍵情報を用いて前記ダウンロード用署名情報を生成する請求項16に記載の認証用装置。

【請求項17】前記半導体回路へのダウンロードを許可された前記階層に対応する第1のアクセス原鍵情報、並びに、当該階層の上位の単数または複数の階層にそれぞれ対応した単数または複数の第2のアクセス原鍵情報を記憶し、

前記第1のアクセス原鍵情報、並びに前記単数または複数の第2のアクセス原鍵情報を用いて前記ダウンロード用署名情報を生成する請求項17に記載の認証用装置。

【請求項18】前記半導体回路との間で相互認証を行った後に、前記ダウンロード用署名情報を前記半導体回路に送信する請求項17に記載の認証用装置。

【請求項19】相互認証用原鍵情報、並びに前記半導体回路の識別情報を記憶し、
前記識別情報を平文として前記相互認証用原鍵情報を用いて暗号化を行って相互認証用鍵情報を生成し、
前記相互認証用鍵情報を用いて前記半導体回路との間で相互認証を行う請求項19に記載の認証用装置。

【請求項20】当該認証用装置に加えられた物理的な外力であって前記アクセス原鍵情報が不正に操作される可能性がある外力を検出した場合に、前記記憶しているアクセス原鍵情報を自動的に消去する請求項16に記載の認証用装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、半導体回路へのプログラムのダウンロードを所定の権限を有する者にのみ認めるデータ処理方法、半導体回路および認証用装置に関する。

【0002】

【従来の技術】現在、ＩＣカードを用いてインターネットなどのネットワークを介した取り引きを行う通信システムが開発されている。このような通信システムでは、決済を行うサーバ装置が、例えばＩＣカードのリーダー・ライターやＰＣ(Personal Computer)からＩＣカードを用いた処理要求を受け、ユーザ認証やデータの暗号化及び復号などの処理を行う。サーバ装置上には、例えば、複数のクレジットカード会社などの事業者のアプリケーションプログラムが動作している。このようなアプリケーションプログラムは、各事業者が作成し、パーソナルコンピュータなどからサーバ装置にダウンロードする。また、各事業者は、アプリケーションプログラムをサーバ装置にダウンロードした後に、必要に応じてデバックなどを行う。

【0003】

【発明が解決しようとする課題】しかしながら、上述したように各事業者がサーバ装置にアプリケーションプログラムをダウンロードしたり、当該アプリケーションプログラムのデバックなどを行う場合に、サーバ装置内のプログラムが不正に改竄等されることを防止する必要がある。これを実現する手法として、例えば、サーバ装置へのアクセスを行う際に、鍵情報を用いた認証処理を行う手法があるが、通常、このような鍵情報は端末装置（上記パーソナルコンピュータ）のメモリに記憶されているため、不正利用される可能性があり、セキュリティ上の問題がある。

【0004】本発明は、上述した従来技術に鑑みてなされたものであり、サーバ装置などの半導体回路へのアクセス内容をその権限に応じて規制できるデータ処理方法、半導体回路および認証用装置を提供することを目的とする。

【0005】

【課題を解決するための手段】上述した目的を達成するために、本発明のデータ処理方法は、半導体回路または当該半導体回路がアクセス可能な半導体記憶装置に、前記半導体回路内で動作するプログラムをダウンロードするデータ処理方法であって、前記半導体回路が複数の階層からなるソフトウェア構造を有し、各階層に対応したダウンロード用署名検証鍵情報を前記半導体回路が参照可能であり、前記半導体回路がダウンロード要求を受けると、当該ダウンロード要求に対応して生成されたダウンロード用署名情報を、前記ダウンロード用署名検証鍵情報を用いて検証し、前記ダウンロード用署名情報が正当であると検証したことを条件に、当該検証に用いたダ

ウンロード用署名検証鍵情報に対応した階層プログラムのダウンロードを、前記ダウンロード要求の発行元に許可する。

【0006】また、本発明のデータ処理方法は、好ましくは、認証用装置が、ダウンロードが許可されるプログラムが属する階層に対応したアクセス原鍵情報を記憶し、前記認証用装置が、前記半導体回路に前記ダウンロード要求を送信し、前記認証用装置が、当該アクセス原鍵情報を用いて前記ダウンロード用署名情報を生成し、当該ダウンロード用署名情報を前記半導体回路に送信する。

【0007】また、本発明のデータ処理方法は、好ましくは、前記認証用装置が、前記半導体回路の識別情報を記憶し、前記認証用装置が、前記識別情報を平文として前記アクセス原鍵情報を用いて暗号化を行ってダウンロード用源鍵情報を生成し、当該ダウンロード用原鍵情報を用いて前記ダウンロード用署名情報を生成する。

【0008】また、本発明のデータ処理方法は、好ましくは、前記認証用装置が、前記半導体回路へのダウンロードを許可された前記階層に対応する第1のアクセス原鍵情報、並びに、当該階層の上位の単数または複数の階層にそれぞれ対応した単数または複数の第2のアクセス原鍵情報を記憶し、前記認証用装置が、前記第1のアクセス原鍵情報、並びに前記単数または複数の第2のアクセス原鍵情報を用いて前記ダウンロード用署名情報を生成する。

【0009】また、本発明のデータ処理方法は、好ましくは、前記認証用装置は、前記半導体回路との間で相互認証を行った後に、前記ダウンロード用署名情報を前記半導体回路に送信する。

【0010】また、本発明のデータ処理方法は、好ましくは、前記認証用装置が、相互認証用原鍵情報、並びに前記半導体回路の識別情報を記憶し、前記認証用装置が、前記識別情報を平文として前記相互認証用原鍵情報を用いて暗号化を行って相互認証用鍵情報を生成し、前記認証用装置が、前記相互認証用鍵情報を用いて前記半導体回路との間で相互認証を行う。

【0011】また、本発明のデータ処理方法は、好ましくは、前記半導体回路のソフトウェア構造が、前記半導体回路の管理者にのみダウンロード権が与えられた第1の階層と、前記第1の階層の上位に位置し所定の集積回路を操作するプログラムが属する第2の階層と、前記第2の階層の上位に位置し前記集積回路を用いた取り引き手続き内容を規定したアプリケーションプログラムが属する第3の階層とに分類されている。

【0012】また、本発明のデータ処理方法は、好ましくは、前記集積回路は、カードに搭載されており、前記半導体回路は、通信回線、並びに当該通信回線に接続された通信装置を介して前記集積回路にアクセスを行う。

【0013】また、本発明のデータ処理方法は、好ましくは、前記第3の階層には、前記集積回路を用いた取り引きを行う複数の事業者のそれぞれに対応したアプリケーションプログラムが属し、当該複数のアプリケーションプログラムのそれぞれにファイアウォールが規定されており、前記ファイアウォールを介した前記アプリケーションプログラム間のデータ授受またはデータ参照が規制されている。

【0014】また、本発明のデータ処理方法は、好ましくは、前記認証用装置は、当該認証用装置に加えられた物理的な外力であって前記アクセス原鍵情報が不正に操作される可能性がある外力を検出した場合に、前記記憶しているアクセス原鍵情報を自動的に消去する。

【0015】また、本発明の半導体回路は、複数の階層からなるソフトウェア構造を有する半導体回路であって、各階層に対応したダウンロード用署名検証鍵情報を参照可能であり、ダウンロード要求を受けると、当該ダウンロード要求に対応して生成されたダウンロード用署名情報を、前記ダウンロード用署名検証鍵情報を用いて検証し、前記ダウンロード用署名情報が正当であると検証したことを条件に、当該検証に用いたダウンロード用署名検証鍵情報に対応した階層のプログラムを、当該半導体回路または当該半導体回路にアクセス可能な半導体記憶回路にダウンロードすることを、前記ダウンロード要求の発行元に許可する。

【0016】また、本発明の認証用装置は、複数の階層からなるソフトウェア構造を有する半導体回路または当該半導体回路がアクセス可能な半導体記憶装置に、前記半導体回路内で動作するプログラムをダウンロードする際の認証に用いられる認証用装置であって、前記ダウンロードが許可されるプログラムが属する前記階層に対応したアクセス原鍵情報を記憶し、前記半導体回路に前記ダウンロード要求を送信し、当該アクセス原鍵情報を用いて前記ダウンロード用署名情報を生成し、当該ダウンロード用署名情報を前記半導体回路に送信する。

【0017】

【発明の実施の形態】以下、本発明の実施の形態を添付図面を参照して説明する。図1は、本実施形態の通信システム301の全体構成図である。図1に示すように、通信システム301は、サーバ装置302、ICカード303（本発明の集積回路）、カードリーダ・ライタ304、パーソナルコンピュータ305、ASP (Application Service Provider)サーバ装置106、SAM (Secure Application Module) ユニット309、パーソナルコンピュータ316_1、316_2、316_3、316_4、316_5、認証用ユニット317_1、317_2、317_3、317_4、317_5（本発明の認証用装置）、並びにICE (In Circuit Emulator) 318を用いて、インターネット310を介して通信を行って、SAMチップ308のソフトウェアの開発やカスタマイズ、並びにICカード303を用いた決済

処理などを行う。SAMユニット309は、外部メモリ307（本発明の半導体記憶回路）およびSAMチップ308（本発明の半導体回路）を有する。SAMチップ308は、図2に示すようなソフトウェア構成を有している。図2に示すように、SAMチップ308は、下層から上層に向けて、HW(Hardware)層、OS層、下位ハンドラ層、上位ハンドラ層およびアプリケーション(AP)層を順に有している。下位ハンドラ層は、アプリケーションプログラムに依存しない処理を規定する層であり、OSIプロトコルにおけるトランスポート層、ネットワーク層およびデータリンク層に対応している。下位ハンドラ層には、ドライバ層が含まれる。ドライバ層は、LSIの操作に係わる処理を行う層である。上位ハンドラ層は、アプリケーションプログラムに依存する処理を規定する層であり、OSIプロトコルにおけるトランスポート層より上の層に対応している。ここで、OS層が本発明の第1の層に対応し、下位ハンドラ層、ドライバ層および上位ハンドラ層が本発明の第2の層に対応し、AP層が本発明の第3の層に対応している。

【0018】AP層には、図1に示すクレジットカード会社などの事業者315_1、315_2、315_3によるICカード303を用いた手続きを規定したアプリケーションプログラムAP_1、AP_2、AP_3がある。AP層では、アプリケーションプログラムAP_1、AP_2、AP_3相互間、並びに上位ハンドラ層との間にファイアウォールFW（本発明のファイアウォール）が設けられている。

【0019】図2に示すソフトウェア構造において、AP層で各事業者に特有の処理、例えばICカード303を用いた決済処理の内容が規定されており、ICカード303を直接操作する処理は上位ハンドラ層以下の層に規定されている。

【0020】SAMチップ308は、SCSIまたはEthernetなどを介してASPサーバ装置306に接続される。ASPサーバ装置306は、インターネット310を介して、パーソナルコンピュータ305、316_1、316_2、316_3、316_4、316_5が接続されている。

【0021】パーソナルコンピュータ316_1は、SAMチップ308で実行されるアプリケーションプログラムAP_1の事業者315_AP1が使用する。パーソナルコンピュータ316_2は、SAMチップ308で実行されるアプリケーションプログラムAP_2の事業者315_AP2が使用する。パーソナルコンピュータ316_3は、SAMチップ308で実行されるアプリケーションプログラムAP_3の事業者315_AP3が使用する。パーソナルコンピュータ316_4は、SAMチップ308の図2に示す上位ハンドラ層、並びにドライバ層を含む下位ハンドラ層を開発可能なソフトウェア開発者315_MIDが使用する。パーソナルコ

ンピュータ316_5は、SAMチップ308の製造元であり、SAMチップ308を統括して管理する権限を有するソフトウェア開発者315_SUPが使用する。

【0022】事業者315_AP1、315_AP2、315_AP3は、パーソナルコンピュータ316_1、316_2、316_3を用いてアプリケーションプログラムAP_1、AP_2、AP_3を作成し、それぞれ認証用ユニット317_1、317_2、317_3を介して、当該作成したアプリケーションプログラムをSAMチップ308を介して外部メモリ307内の予め割り当てられた記憶領域にダウンロードする。このとき、事業者315_AP1、315_AP2、315_AP3は相互に無関係の者であるため、アプリケーションプログラムAP_1、AP_2、AP_3をダウンロードできる外部メモリ307内の記憶領域は予め決められており、当該記憶領域へのダウンロードを行う権限を有するか否かがSAMチップ308によって検証される。また、アプリケーションプログラムAP_1、AP_2、AP_3の実行中は、ファイアウォールFWによって、アプリケーションプログラムAP_1、AP_2、AP_3の間でのデータの授受および参照が制限されている。

【0023】ソフトウェア開発者315_MIDは、認証用ユニット317_4を介して、必要に応じて、SAMチップ308の図2に示す上位ハンドラ層、並びにドライバ層を含む下位ハンドラ層のカスタマイズ等のために所定のプログラムをSAMチップ308にダウンロードする。

【0024】ソフトウェア開発者315_SUPは、認証用ユニット317_5を介して、図2に示す全ての層のカスタマイズ等のために所定のプログラムをSAMチップ308にダウンロードする。

【0025】認証用ユニット317_1～317_5は、後述するように、それぞれパーソナルコンピュータ316_1～316_5から所定のプログラムをSAMチップ308にダウンロードする際に、SAMチップ308との間で相互認証、並びにダウンロード用署名検証鍵情報の作成などを行う。

【0026】パーソナルコンピュータ305は、例えば、ICカード303の所有者であるエンドユーザが使用する。パーソナルコンピュータ305は、例えば、シリアルまたはUSBを介してDumb型のカードリーダー・ライタ304に接続されている。カードリーダー・ライタ304が、ICカード303との間で物理レベルに相当する例えば無線通信を実現する。ICカード303への操作コマンドおよびICカード303からのレスポンスパケットは、SAMユニット309側で生成および解読される。よって、その中間に介在するカードリーダー・ライタ304、パーソナルコンピュータ305およびASPサーバ装置306は、コマンドやレスポンス内容を

データペイロード部分に格納して中継する役割を果たすのみで、ICカード303内のデータの暗号化や復号および認証などの実操作には関与しない。また、ICE318は、SAMチップ308上で動作するプログラムをデバックする際に用いられるエミュレータである。

【0027】以下、図1に示す構成要素について説明する。

ICカード303

ICカード303は、SAMチップ308を用いた決済処理に必要な鍵情報などを記憶する。

【0028】認証用ユニット317_1～317_5、図3は、認証用ユニット317_1の機能ブロック図である。図3に示すように、認証用ユニット317_1は、記憶部350_1および処理部351_1を有する。図3に示すように、記憶部350_1は、SAM_ID、相互認証用原鍵情報K1およびアクセス原鍵情報KAを記憶している。SAM_IDは、SAMチップ308の識別情報である。相互認証用原鍵情報K1は、後述するように相互認証用鍵情報K2を生成するために用いられる。アクセス原鍵情報KAは、後述するように、外部メモリ307にプログラムをダウンロードするときに用いられるダウンロード用署名情報を生成するために用いられる。アクセス原鍵情報KAは、図2に示すSAMチップ308のソフトウェア構造のAP層のプログラムを外部メモリ307にダウンロードするために必要な鍵情報である。

【0029】処理部351_1は、図3に示すように、相互認証部352_1およびダウンロード処理部353_1を有する。相互認証部352_1は、図4に示すように、プログラムを外部メモリ307にダウンロードする際に、SAM_IDを平文として相互認証用原鍵情報K1を用いて暗号化を行って相互認証用鍵情報K2を生成し、当該相互認証鍵情報K2を用いてSAMチップ308との間で相互認証を行う。ダウンロード処理部353_1は、プログラムを外部メモリ307にダウンロードする際に、図5に示すように、SAM_IDを平文としてアクセス原鍵情報KAを用いて暗号化を行って、ダウンロード用鍵情報K_DAを生成する。また、ダウンロード処理部353_1は、ダウンロード用鍵情報K_DAを用いてダウンロード用署名情報を生成し、これをSAMチップ308に送信する。

【0030】認証用ユニット317_2、317_3は、上述した認証用ユニット317_1と同じ構成をしている。但し、例えば、アクセス原鍵情報KAの内容は各認証用ユニットで異なる。

【0031】図6は、認証用ユニット317_4の機能ブロック図である。図6に示すように、認証用ユニット317_4は、記憶部350_4および処理部351_4を有する。図6に示すように、記憶部350_4は、SAM_ID、相互認証用原鍵情報K1およびアクセス

原鍵情報KA、KMを記憶している。SAM_ID、相互認証用原鍵情報K1およびアクセス原鍵情報KAは、前述したものと同一である。アクセス原鍵情報KMは、図2に示すSAMチップ308のソフトウェア構造の上位ハンドラ層、並びにドライバ層を含む下位ハンドラ層のプログラムを外部メモリ307あるいはSAMチップ308にダウンロードするために必要な鍵情報である。

【0032】処理部351_4は、図6に示すように、相互認証部352_4およびダウンロード処理部353_4を有する。相互認証部352_4は、前述した図4に相互認証部352_1と同じである。ダウンロード処理部353_4は、プログラムを外部メモリ307にダウンロードする際に、図7に示すように、SAM_IDを平文としてアクセス原鍵情報KAを用いて暗号化を行って、ダウンロード用鍵情報K_DAを生成する。次に、ダウンロード処理部353_4は、ダウンロード用鍵情報K_DAを平文としてアクセス原鍵情報KMを用いて暗号化を行って、ダウンロード用鍵情報K_DMを生成する。次に、ダウンロード処理部353_4は、ダウンロード用鍵情報K_DMを用いてダウンロード用署名情報を生成し、これをSAMチップ308に送信する。

【0033】図8は、認証用ユニット317_5の機能ブロック図である。図8に示すように、認証用ユニット317_5は、記憶部350_5および処理部351_5を有する。図8に示すように、記憶部350_5は、SAM_ID、相互認証用原鍵情報K1およびアクセス原鍵情報KA、KM、KSを記憶している。SAM_ID、相互認証用原鍵情報K1およびアクセス原鍵情報KA、KMは、前述したものと同一である。アクセス原鍵情報KSは、図2に示すSAMチップ308のソフトウェア構造のOS層のプログラムを外部メモリ307あるいはSAMチップ308にダウンロードするために必要な鍵情報である。

【0034】処理部351_5は、図8に示すように、相互認証部352_5およびダウンロード処理部353_5を有する。相互認証部352_5は、前述した図4に相互認証部352_1と同じである。ダウンロード処理部353_5は、プログラムを外部メモリ307にダウンロードする際に、図9に示すように、SAM_IDを平文としてアクセス原鍵情報KAを用いて暗号化を行って、ダウンロード用鍵情報K_DAを生成する。次に、ダウンロード処理部353_5は、ダウンロード用鍵情報K_DAを平文としてアクセス原鍵情報KMを用いて暗号化を行って、ダウンロード用鍵情報K_DMを生成する。次に、ダウンロード処理部353_5は、ダウンロード用鍵情報K_DMを平文としてアクセス原鍵情報KSを用いて暗号化を行って、ダウンロード用鍵情報K_DSを生成する。次に、ダウンロード処理部353_5は、ダウンロード用鍵情報K_DSを用いてダウ

ンロード用署名情報を生成し、これをSAMチップ308に送信する。

【0035】本実施形態では、認証用ユニット317_1, 317_4, 317_5は、記憶部350_1, 350_4, 350_5内にセキュアな状態で情報を記憶しており、当該ユニットが外的な要因で破壊されたり、こじ開けられた場合には、そのことを検出部によって検出して、記憶部350_1, 350_4, 350_5の記憶情報を消去する。

【0036】SAMユニット309

〔外部メモリ307〕図10は、外部メモリ307の記憶領域を説明するための図である。図10に示すように、外部メモリ307の記憶領域には、事業者315_1のアプリケーションプログラムAP_1が記憶されるAP記憶領域320_1、事業者315_2のアプリケーションプログラムAP_2が記憶されるAP記憶領域320_2、事業者315_3のアプリケーションプログラムAP_3が記憶されるAP記憶領域320_3、並びにSAMチップ308の管理者が使用するAP管理用記憶領域321がある。

【0037】AP記憶領域320_1に記憶されているアプリケーションプログラムAP_1は、複数のプログラムモジュールによって構成されている。AP記憶領域320_1へのアクセスは、ファイアウォールFW_1によって制限されている。AP記憶領域320_2に記憶されているアプリケーションプログラムAP_2は、複数のプログラムモジュールによって構成されている。AP記憶領域320_2へのアクセスは、ファイアウォールFW_2によって制限されている。AP記憶領域320_3に記憶されているアプリケーションプログラムAP_3は、複数のプログラムモジュールによって構成されている。AP記憶領域320_3へのアクセスは、ファイアウォールFW_3によって制限されている。本実施形態では、上記プログラムモジュールは、例えば、SAMユニット309の外部から外部メモリ307にダウンロードされる最小単位である。各アプリケーションプログラムを構成するプログラムモジュールの数は、対応する事業者が任意に決定できる。

【0038】また、外部メモリ307に記憶されたアプリケーションプログラムAP_1, AP_2, AP_3は、スクランブルされており、SAMチップ308に読み込まれたときに、デスクランブルされる。また、アプリケーションプログラムAP_1, AP_2, AP_3は、例えば、それぞれ図1に示すパーソナルコンピュータ316_1, 316_2, 316_3を用いて、事業者315_1, 315_2, 315_3によって作成され、SAMチップ308を介して外部メモリ307にダウンロードされる。

【0039】AP管理用記憶領域321へのアクセスは、ファイアウォールFW_4によって制限されてい

る。なお、ファイアウォールFW_1, FW_2, FW_3, FW_4は、図2に示すファイアウォールFWに対応している。AP管理用記憶領域321には、AP管理用データ330が記憶されている。AP管理用データ330には、例えば、SAM_ID、相互認証用鍵情報K2（または相互認証用原鍵情報K1）、ダウンロード用署名検証鍵情報K_DVA, KDVM, KDVSがある。ここで、ダウンロード用署名検証鍵情報K_DVAは、ダウンロード用鍵情報K_DAを用いて生成された署名情報の正当性を検証する鍵情報である。ダウンロード用署名検証鍵情報K_DVMは、ダウンロード用鍵情報K_DMを用いて生成された署名情報の正当性を検証する鍵情報である。ダウンロード用署名検証鍵情報K_DVSは、ダウンロード用鍵情報K_DSを用いて生成された署名情報の正当性を検証する鍵情報である。

【0040】ダウンロード用署名検証鍵情報は、当該プログラムモジュールをSAMチップ308を介して外部メモリ307にダウンロードするときに行われる署名検証に用いられる鍵情報である。

【0041】〔SAMチップ308〕図11は、図1に示すSAMチップ308の機能ブロック図である。図11に示すように、SAMチップ308は、ASPS通信インタフェース部360、外部メモリ通信インタフェース部361、バススクランブル部362、暗号・復号部363、記憶部364およびCPU365を有する。SAMチップ308は、耐タンパ性のモジュールである。

【0042】ASPS通信インタフェース部360は、図1に示すASPサーバ装置306との間のデータ入出力に用いられるインタフェースである。外部メモリ通信インタフェース部361は、外部メモリ307との間のデータ入出力に用いられるインタフェースである。バススクランブル部362は、外部メモリ通信インタフェース部361を介してデータを外部メモリ307との間で入出力する際に、出力するデータをスクランブルし、入力したデータをデスクランブルする。暗号・復号部363は、データの暗号化、並びに暗号化されたデータの復号を行う。記憶部364は、CPU365の処理に用いられるデータを記憶する。CPU365は、SAMチップ308が行うアプリケーションプログラムの実行を含む様々を処理を、タスクなどの形態で処理を行う。CPU365は、例えば、インターネット310を介したプログラムモジュールのダウンロード処理を行うダウンロード用タスク365aを実行する。

【0043】以下、CPU365のダウンロード用タスク365aによるプログラムモジュールのダウンロード動作について説明する。図12は、当該ダウンロード動作を説明するためのフローチャートである。以下の実施形態では、事業者315_AP1が、図2および図10に示すアプリケーションプログラムAP_1のプログラムモジュールをダウンロードする場合の動作を例に挙げ

て説明する。

ステップST301：図1に示すパーソナルコンピュータ316_1が、認証用ユニット317_1、インターネット310、ASPサーバ装置306およびICE318を介して、アプリケーションプログラムAP_1を構成するダウンロードを行おうとするプログラムモジュールのモジュール名を指定したダウンロード要求をSAMチップ308に送信する。

【0044】ステップST302：認証用ユニット317_1の処理部351_1の相互認証部352_1が、図4に示すように、SAM_IDを平文として相互認証用原鍵情報K1を用いて暗号化を行って相互認証用鍵情報K2を生成する。

【0045】ステップST303：認証用ユニット317_1の処理部351_1の相互認証部352_1が、SAMチップ308のCPU365のダウンロード用タスク365aとの間で、ステップST302で生成した相互認証用鍵情報K2を用いて相互認証を行う。

【0046】ステップST304：ステップST303の相互認証においてお互いの正当性が確認されると、ステップST305の処理に進む、そうでない場合には処理を終了する。

【0047】ステップST305：図3に示す認証用ユニット317_1の処理部351_1のダウンロード処理部353_1が、図5に示すように、SAM_IDを平文としてアクセス原鍵情報KAを用いて暗号化を行って、ダウンロード用鍵情報K_DAを生成する。

【0048】ステップST306：ダウンロード処理部353_1が、ステップST305で生成したダウンロード用鍵情報K_DAを用いてダウンロード用署名情報を生成する。

【0049】ステップST307：ダウンロード処理部353_1が、ステップST306で生成したダウンロード用署名情報をSAMチップ308に送信する。

【0050】ステップST308：図11に示すSAMチップ308のCPU365のダウンロード用タスク365aが、図10に示すダウンロード用署名検証鍵情報K_DVAを用いて、ステップST307で受信したダウンロード用署名情報の正当性を判断する。このとき、ダウンロード用タスク365aは、ステップST301で受信したモジュール名に基づいて、ダウンロード要求がAP層について行われたと判断し、ダウンロード用署名検証鍵情報K_DVAを特定する。

【0051】ステップST309：ステップST308においてダウンロード用署名情報が正当であると判断されると、ステップST310の処理に進む、そうでない場合には処理を終了する。

【0052】ステップST310：図11に示すSAMチップ308のCPU365のダウンロード用タスク365aが、ステップST301で指定されたモジュール

名に対応する外部メモリ307内のアドレスをモジュール管理用データ330を参照して特定し、当該特定した外部メモリ307上のアドレスに、パーソナルコンピュータ316_1から受信したプログラムモジュールをダウンロードする。

【0053】なお、ソフトウェア開発者315_MIDが、図2に示す上位ハンドラ層および下位ハンドラ層のプログラムモジュールを外部メモリ307にダウンロードする場合には、ステップST305において図7を用いて説明した手順でダウンロード用鍵情報K_DMが生成され、これを用いてステップST306でダウンロード用署名情報が生成される。また、ステップST308で、SAMチップ308内で、図10に示すダウンロード用署名検証鍵情報K_DVMを用いて、ダウンロード用署名情報の検証が行われる。また、ソフトウェア開発者315_SUPが、図2に示すOS層のプログラムモジュールを外部メモリ307にダウンロードする場合には、ステップST305において図9を用いて説明した手順でダウンロード用鍵情報K_DSが生成され、これを用いてステップST306でダウンロード用署名情報が生成される。また、ステップST308で、SAMチップ308内で、図10に示すダウンロード用署名検証鍵情報K_DVSを用いて、ダウンロード用署名情報の検証が行われる。

【0054】なお、ソフトウェア開発者315_MID、315_SUPは、アクセス原鍵情報KAを用いて、AP層のプログラムモジュールを外部メモリ307にダウンロードできる。また、ソフトウェア開発者315_SUPは、アクセス原鍵情報KA、KMを用いて上位ハンドラ層および下位ハンドラ層のプログラムモジュールを外部メモリ307にダウンロードできる。

【0055】以下、図1に示す通信システム301によるICカード303を用いた取り引き処理について説明する。図13は、図1に示す通信システム301の全体動作を説明するための図である。

ステップST331：事業者315_1～315_3あるいはこれら事業者の依頼を受けた者が、当該事業者がICカード303を用いて行う取り引きについての処理を行うためのアプリケーションプログラムAP_1、AP_2、AP_3を、図1に示すパーソナルコンピュータ316_1、316_2、316_3上で作成する。このとき図12を用いて説明したダウンロード処理が行われる。

【0056】ステップST332：アプリケーションプログラムAP_1、AP_2、AP_3を、認証用ユニット317_1、317_2、317_3を介して、パーソナルコンピュータ316_1、316_2、316_3からSAMチップ308にダウンロードする。このとき、図9を用いて説明した処理が行われる。

【0057】ステップST333：ユーザにICカード

303が発行される。ICカード303には、ユーザが契約を行った事業者との取り引きに用いられる鍵情報が記憶されている。なお、ユーザと事業者との間の契約は、ICカード303の発行後に、インターネット310などを介して行ってもよい。

【0058】ステップST334：例えば、ユーザがパーソナルコンピュータ305を用いてインターネット310を介してサーバ装置302にアクセスを行い、商品を購入しようとした場合に、サーバ装置302がインターネット310を介してASPサーバ装置306に処理要求を出す。ASPサーバ装置306は、サーバ装置302から処理要求を受けると、インターネット310を介してパーソナルコンピュータ305にアクセスを行う。そして、カードリーダー・ライタ304が出したICカード303についての処理要求が、パーソナルコンピュータ305、インターネット310およびASPサーバ装置306を介してSAMチップ308に送信される。

【0059】ステップST335：SAMチップ308が、ステップST334で受信した処理要求に応じて、決済処理手順タスクによってアプリケーションプログラムを選択し、当該選択されたアプリケーションプログラムを実行する。

【0060】ステップST336：SAMチップ308は、アプリケーションプログラムの実行結果をASPサーバ装置306に出力する。

【0061】以上説明したように、通信システム301によれば、認証用ユニット317_1、317_2、317_3がアクセス原鍵情報KAを保持し、認証用ユニット317_4がアクセス原鍵情報KMを保持し、認証用ユニット317_5がアクセス原鍵情報KSを保持し、上述したように外部メモリ307へのプログラムモジュールのダウンロード処理を行うことで、図2に示すソフトウェア階層に応じて与えた権限に応じたプログラムモジュールのダウンロードが可能になる。そのため、権限の無い者によって、SAMチップ308で実行されるプログラムモジュールが不正に交換されたり、改竄されることを防止できる。

【0062】また、通信システム301によれば、前述したように、認証用ユニット317_1、317_4、317_5は、記憶部350_1、350_4、350_5内にセキュアな状態で情報を記憶しており、当該ユニットが外的な要因で破壊されたり、こじ開けられた場合には、そのことを検出部によって検出して、記憶部350_1、350_4、350_5の記憶情報を消去する。そのため、SAMチップ308へのダウンロードに用いられる鍵情報が不正に使用されることを回避できる。

【0063】また、通信システム301によれば、SAMチップ308が複数のアプリケーションプログラムを

動作させる場合に、アプリケーションプログラム間でのデータ授受やデータ・コードの参照をファイアウォールFW_1、FW_2、FW_3によって制限することから、各アプリケーションプログラムの処理が、他のアプリケーションプログラムによって不正干渉、改竄されることを防止できる。また、各アプリケーションプログラムの秘匿性を高めることができる。

【0064】また、通信システム301によれば、各アプリケーションプログラムを複数のプログラムモジュールで構成することで、外部メモリ307に対してプログラムモジュール単位でダウンロードを行うことができる。

【0065】また、通信システム301によれば、秘匿性の高いICカード303に対しての操作に用いられる鍵情報を、通常行われるスクランブルに加えて、暗号化して外部メモリ307に格納することで、当該鍵情報のセキュリティレベルを向上できる。

【0066】また、インターネット301によれば、アプリケーションプログラムは、バススクランブル機能によりコードアクセス時に暗号化・復号化を実行しているため、SAMチップ308の処理停止中に、外部メモリ307に記憶されたアプリケーションプログラムが不正に解析等されることを防止できる。

【0067】図14は、図11に示すSAMチップ308の機能ブロックをより具体的に示した機能ブロック図である。図14に示すように、SAMチップ308は、内部バス90を介して、ASPS通信インタフェース部360、外部メモリ通信インタフェース部361、バススクランブル部362、暗号・復号部365、記憶部364およびCPU365が接続されている。

【0068】図14に示すSAMチップ308では、例えば図15に示すように、内部バス90に接続されたカードI/F部91を、SAMチップ308の外部のRF送受信部92に接続し、RF送受信部92のアンテナ92aを介して、ICカード303との間で非接触方式でデータを送受信してもよい。

【0069】本発明は上述した実施形態には限定されない。例えば、上述した実施形態では、パーソナルコンピュータ316_1～316_5からSAMチップ308を介して外部メモリ307にプログラムモジュールをダウンロードする場合を例示したが、本発明は、パーソナルコンピュータ316_1～316_5からSAMチップ308内の記憶部364にプログラムモジュールをダウンロードする場合にも、上述したダウンロード用タスク365aの機能を用いて同様に適用できる。

【0070】また、上述した実施形態では、インターネット310に対してパーソナルコンピュータ316_1～316_5側に認証用ユニット317_1～317_5を設けた場合を例示したが、図16に示すように、認証用ユニット317_1～317_5をSAMチップ3

08内に設け、認証用ユニット317_1～317_5をへのアクセスを対応するパーソナルコンピュータ316_1～316_5に対して許可するようにしてもよい。

【0071】

【発明の効果】以上説明したように、本発明によれば、半導体回路で用いられるプログラムのダウンロードを、ダウンロード元に予め与えられた権限に応じて規定できるデータ処理方法、半導体回路および認証用装置を提供することができる。

【図面の簡単な説明】

【図1】図1は、本発明の実施形態の通信システムの全体構成図である。

【図2】図2は、図1に示すSAMチップのソフトウェア構成を説明するための図である。

【図3】図3は、図1に示すアプリケーションプログラムを使用する事業者の認証用ユニットの機能ブロック図である。

【図4】図4は、図3に示す相互認証部の機能を説明するための図である。

【図5】図5は、図3に示すダウンロード処理部の機能を説明するための図である。

【図6】図6は、図1に示すハンドラ層のソフトウェア開発者の認証用ユニットの機能ブロック図である。

【図7】図7は、図6に示すダウンロード処理部の機能を説明するための図である。

【図8】図8は、図1に示すSAMチップの管理者の認証用ユニットの機能ブロック図である。

【図9】図9は、図8に示すダウンロード処理部の機能

を説明するための図である。

【図10】図10は、図1に示すSAMユニットの外部メモリを説明するための図である。

【図11】図11は、図1に示すSAMチップの機能ブロック図である。

【図12】図12は、図1に示すパーソナルコンピュータから、外部メモリにアプリケーションプログラムをダウンロードする動作を説明するためのフローチャートである。

【図13】図13は、図1に示す通信システムのICカードを用いた取り引き処理を説明するための図である。

【図14】図14は、図11に示すSAMチップの機能ブロックをより具体的に示した機能ブロック図である。

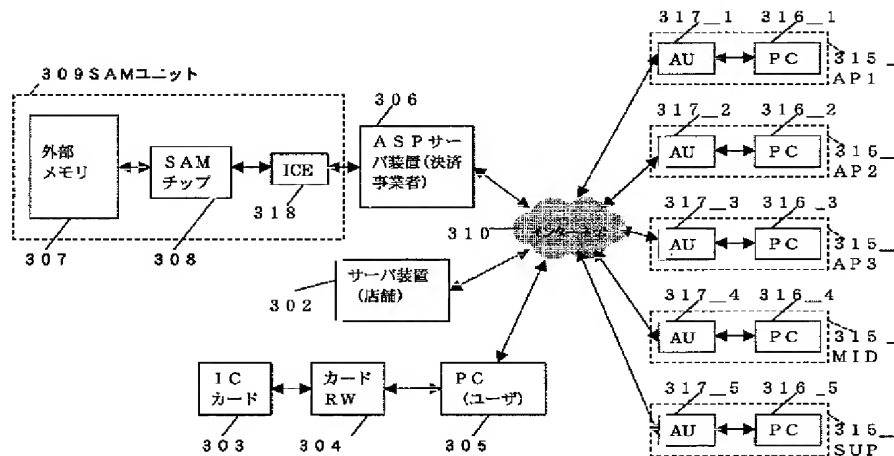
【図15】図15は、SAMチップのその他の使用形態を説明するための図である。

【図16】図16は、図1に示す通信システムの変形例を説明するための図である。

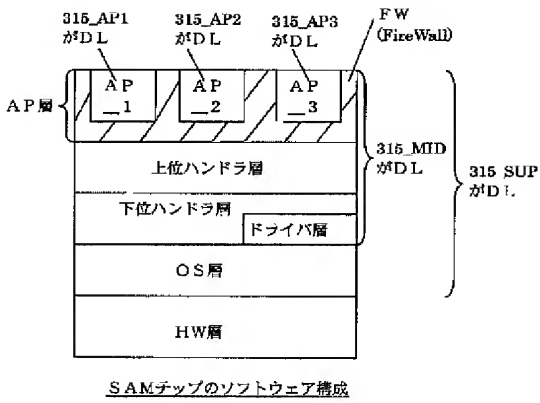
【符号の説明】

301…通信システム、302…サーバ装置、303…ICカード、304…カードリーダー・ライター、305…パーソナルコンピュータ、306…ASPサーバ装置、307…外部メモリ、308…SAMチップ、309…SAMユニット、310…インターネット、315_1, 315_2, 315_3…クレジットカード事業者、315_4…ハンドラ層の開発者、315_5…SAMチップの管理者、316_1～316_5…パーソナルコンピュータ、317_1～317_5…認証用ユニット、318…ICE

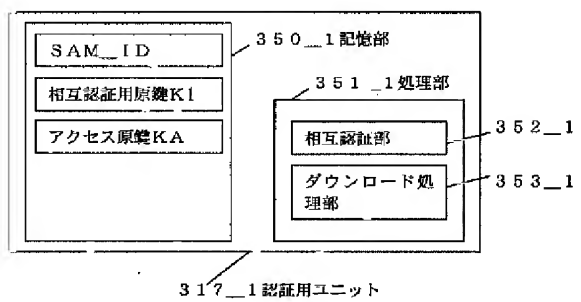
【図1】



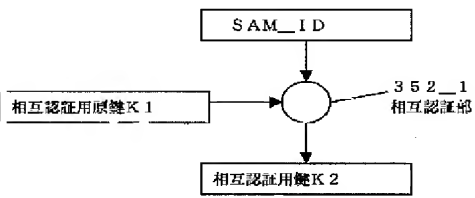
【図2】



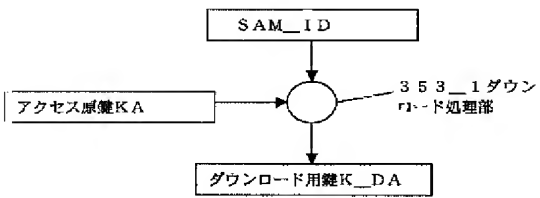
【図3】



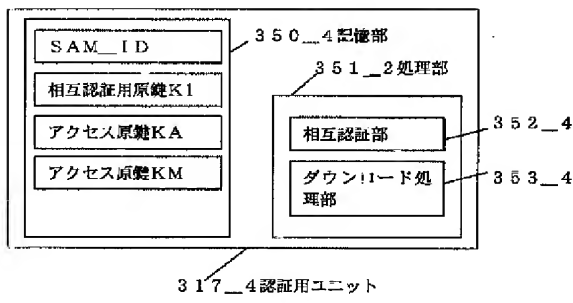
【図4】



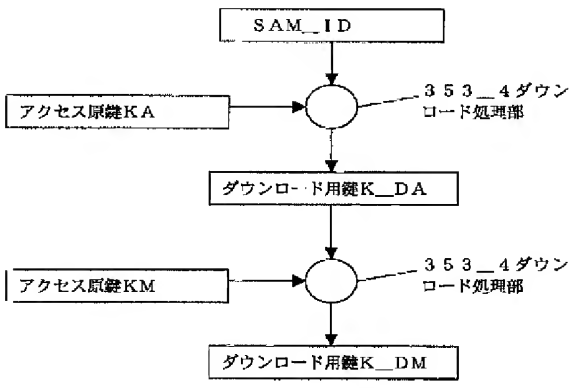
【図5】



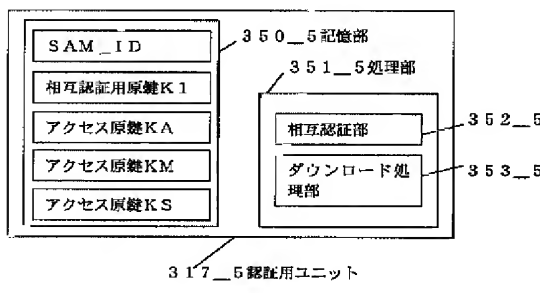
【図6】



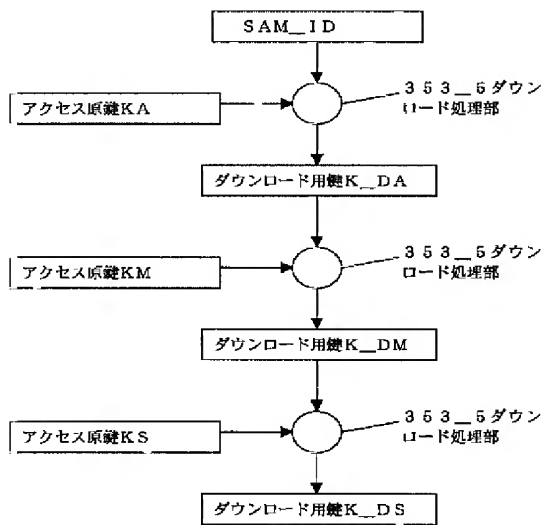
【図7】



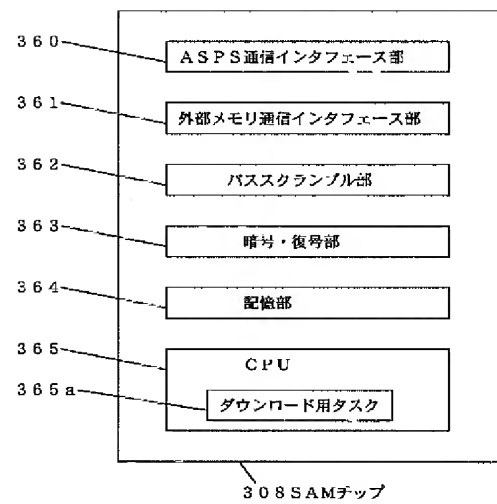
【図8】



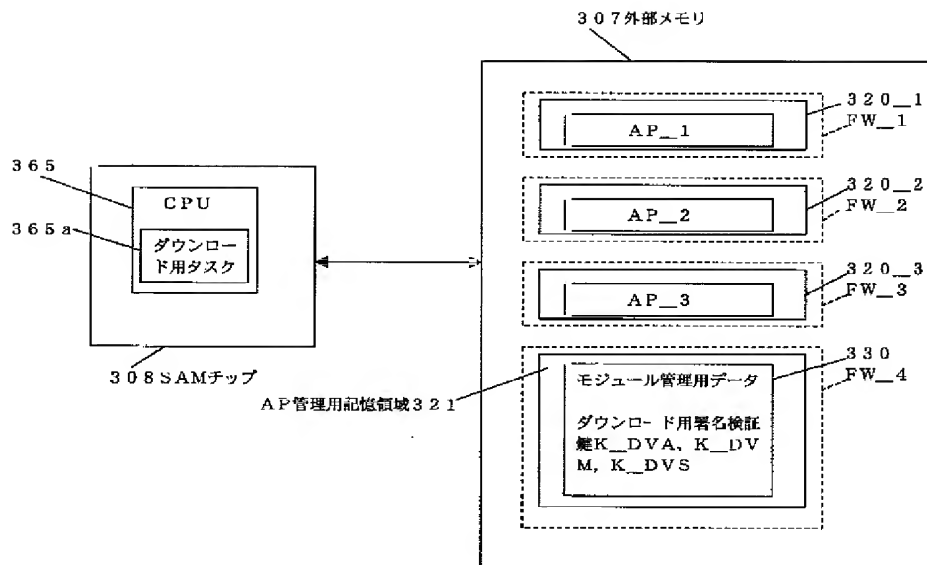
【図9】



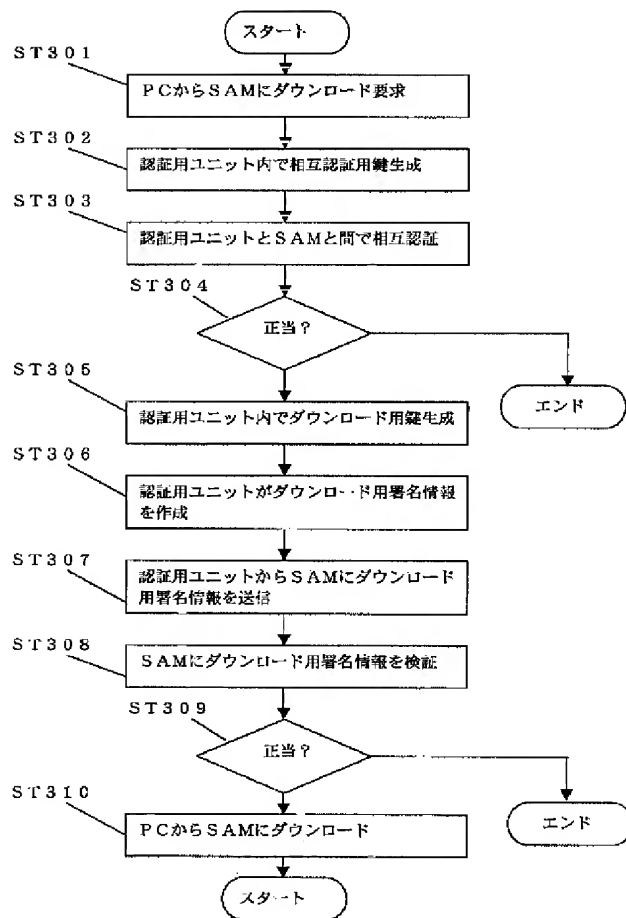
【図11】



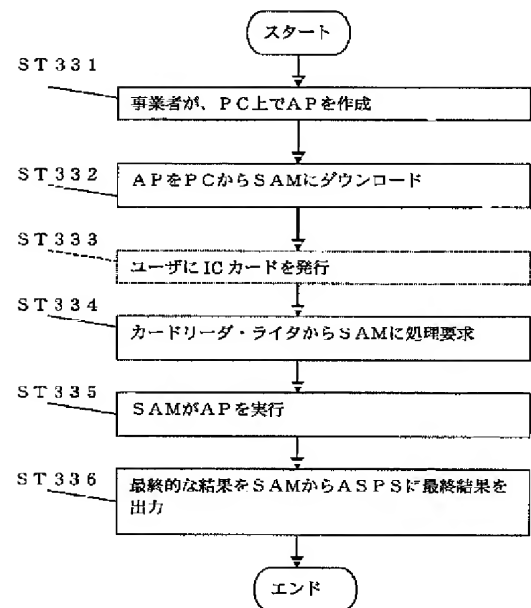
【図10】



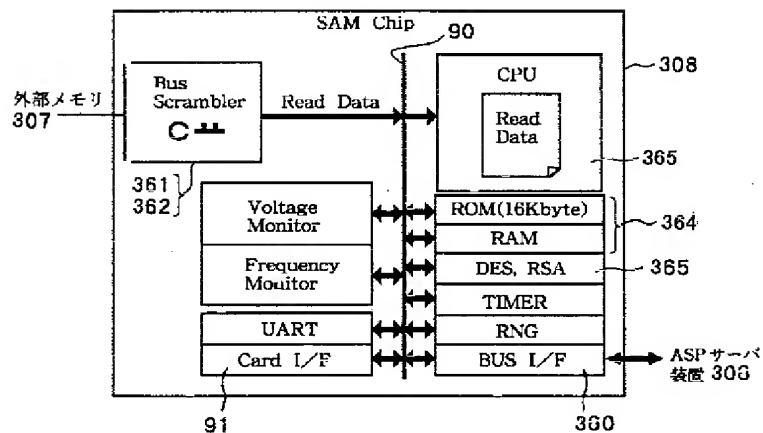
【図12】



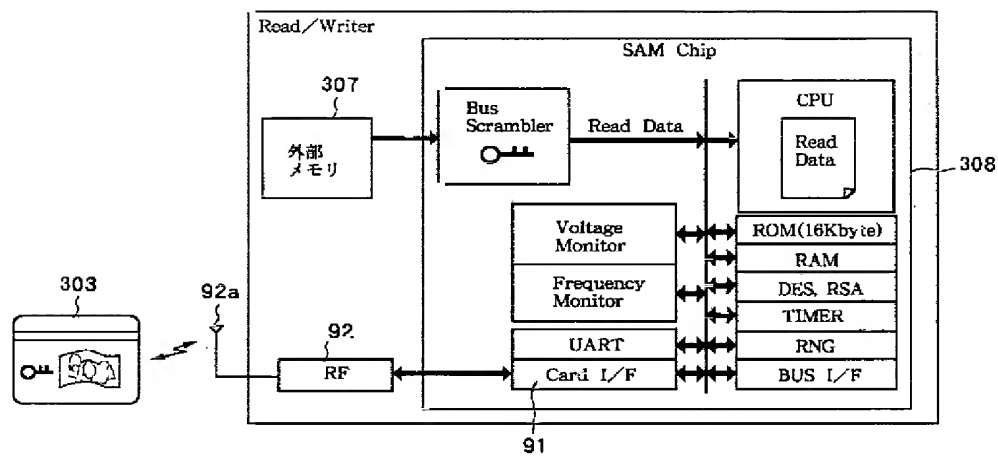
【図13】



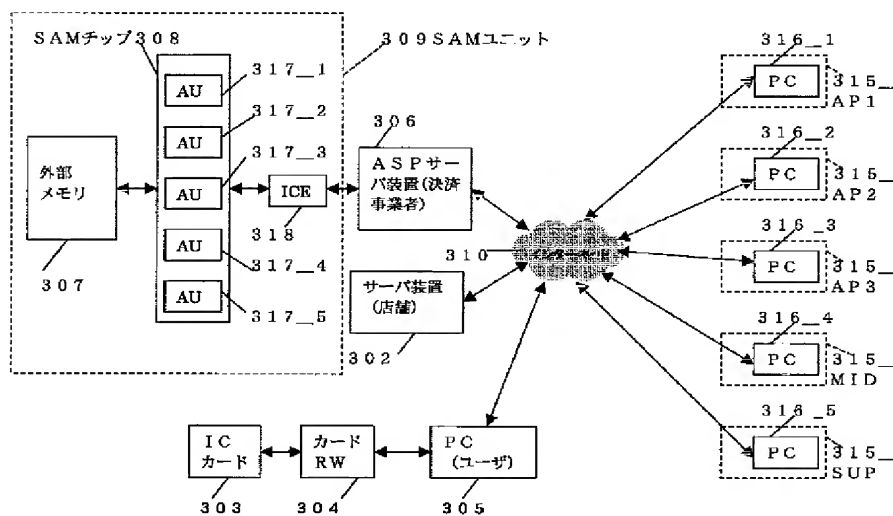
【図14】



【図15】



【図16】



フロントページの続き

(51) Int. Cl.⁷

G 0 9 C 1/00

H 0 4 L 9/10

9/32

識別記号

6 4 0

F I

G 0 6 K 19/00

H 0 4 L 9/00

(参考)

N

P

6 2 1 A

6 7 5 A

Fターム(参考) 5B035 AA13 BB09 CA29 CA38
 5B058 CA26 CA27 KA32 KA33
 5B076 FB05 FC01 FD02
 5J104 AA07 AA09 AA12 KA04 NA02
 NA35 NA41 NA42 PA07 PA10